Plataforma
de inteligência
de ameaças

Kaspersky CyberTrace

kaspersky bring on the future

Kaspersky CyberTrace

Uma plataforma de inteligência de ameaças que integra dados de ameaças com soluções SIEM, ajudando analistas a usar inteligência de ameaças de forma mais eficaz em seus fluxos de trabalho de segurança.

Permitindo a triagem e a análise eficazes de alertas

A quantidade de alertas processados pelos analistas de cibersegurança cresce exponencialmente. Com a análise dessa quantidade de dados, a triagem, a validação e a priorização eficazes de alertas são praticamente impossíveis.

Há vários sinais de alerta vindos de inúmeros produtos de segurança, que fazem com que alertas importantes fiquem perdidos no meio de tanta informação, resultando na sobrecarga dos analistas. SIEMs e outras ferramentas de análise de segurança correlacionam eventos e ajudam a reduzir a quantidade de alertas, mas os analistas de segurança permanecem extremamente sobrecarregados.

Sistemas SIEM

Ao integrar inteligência de ameaças atualizada e legível por máquinas aos controles de segurança existentes, como sistemas SIEM, os profissionais de segurança podem automatizar o processo inicial de triagem, obtendo contexto suficiente para identificar imediatamente alertas que precisam ser investigados ou encaminhados para equipes de resposta a incidentes.

O crescimento contínuo no número de fontes de dados de ameaças e de inteligência de ameaças disponíveis torna difícil para as organizações determinarem quais informações são relevantes para elas. A inteligência de ameaças é fornecida em diferentes formatos e inclui muitos indicadores de comprometimento (IoCs), fazendo com que seja difícil para as SIEMs ou para os controles de segurança de rede assimilá-los.

Integrações

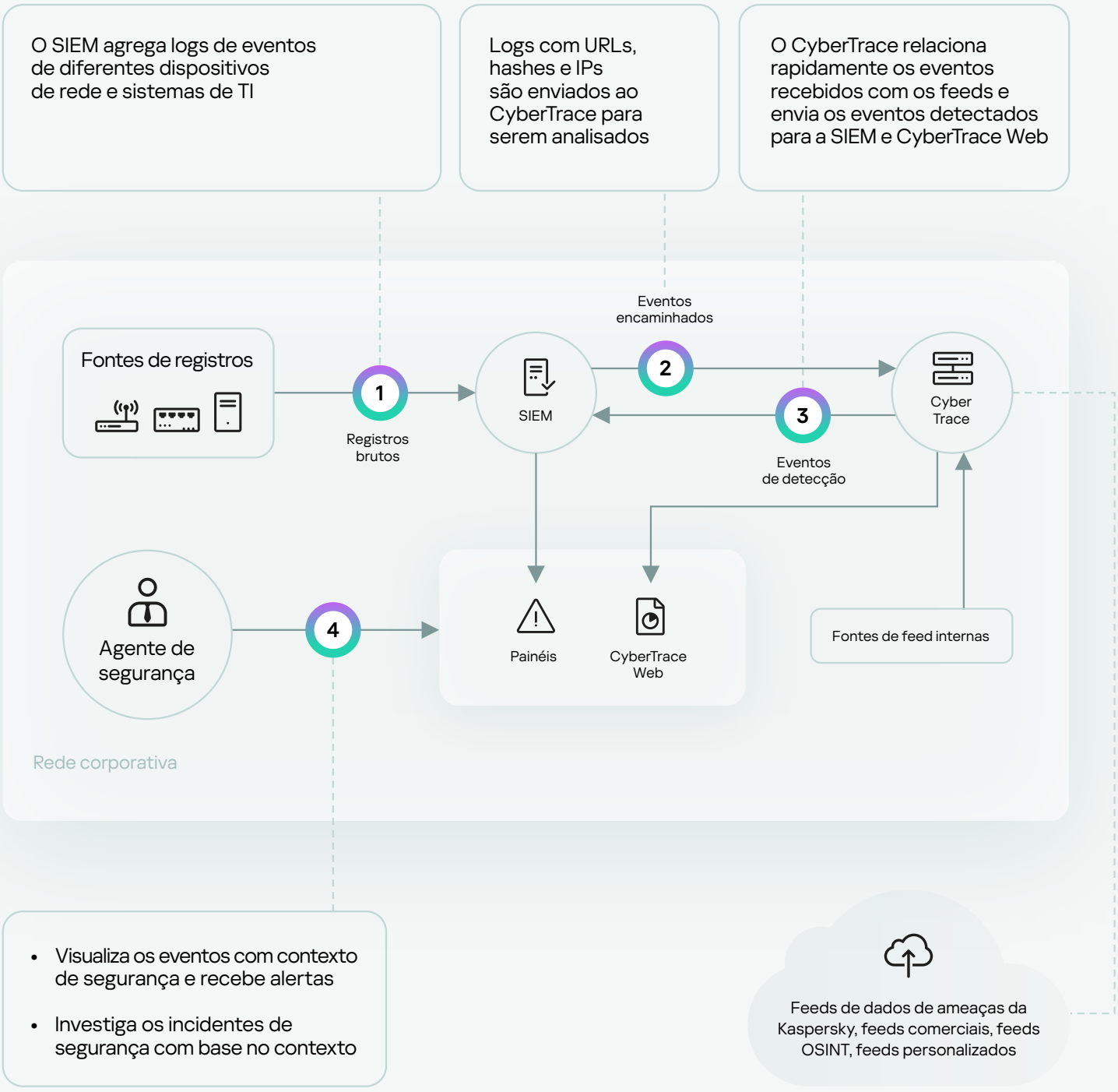
O Kaspersky CyberTrace pode ser integrado a qualquer feed de dados de inteligência contra ameaças nos formatos JSON, STIX, XML e CSV:

1. Dados de inteligência de ameaças da Kaspersky
2. Feeds de dados de outros fornecedores
3. OSINT nos seus feeds personalizados

Para a conveniência dos clientes o CyberTrace é compatível com integração pronta para usar de várias soluções SIEM e fontes de registro.

Esquema de integração do Kaspersky CyberTrace

O Kaspersky CyberTrace pode aprimorar a capacidade do SIEM com uma camada adicional análise e correspondência de dados de entrada, reduzindo significativamente a carga de trabalho do SIEM. Eventos correspondentes com informações de feeds de dados ajudam a identificar ameaças e fornecer contexto valioso para incidentes detectados. Uma arquitetura de alto nível da integração da solução está representada na figura abaixo.



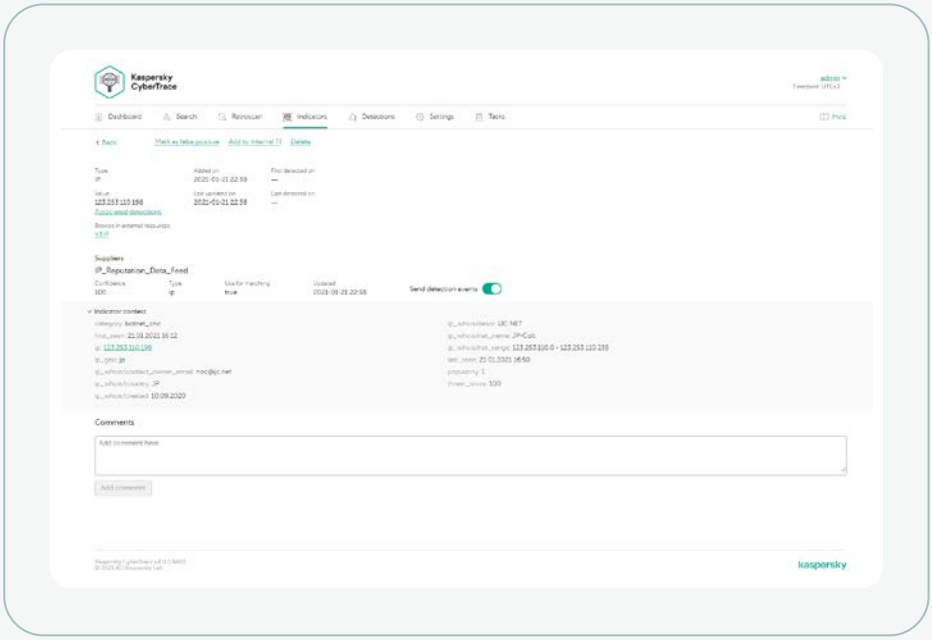
Recursos do produto

O Kaspersky CyberTrace fornece um conjunto de instrumentos para operacionalizar a inteligência de ameaças a fim de realizar uma triagem de alertas e resposta inicial eficazes:

Informações detalhadas sobre um indicador provenientes de todos os fornecedores de inteligência de ameaças

Um banco de dados de indicadores com pesquisa de texto completo e a capacidade de pesquisar usando search queries avançadas permite pesquisas complexas em todos os campos de indicadores, incluindo campos de contexto. A filtragem de resultados por fornecedor de inteligência simplifica o processo de análise da inteligência de ameaças.

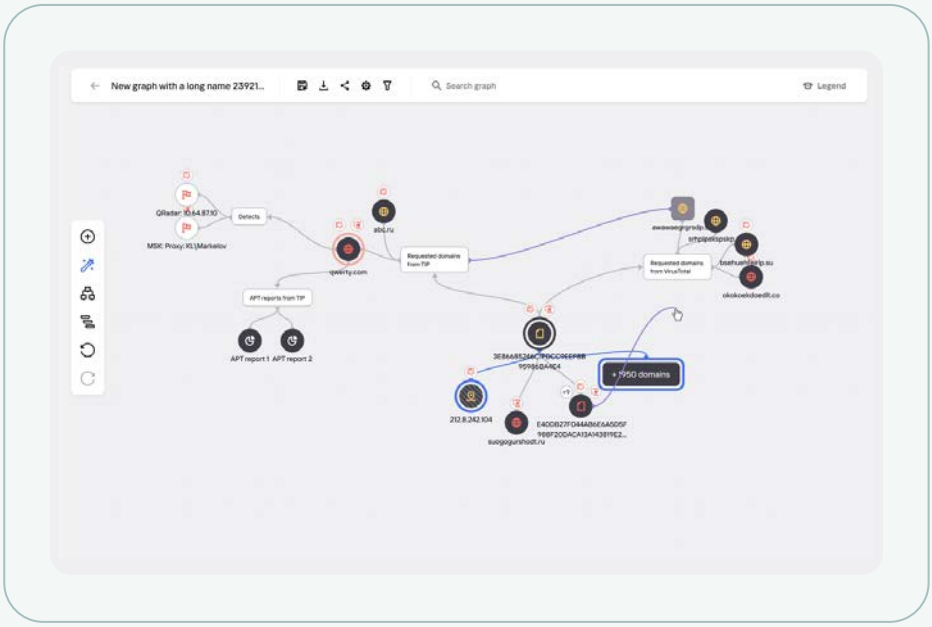
Assinaturas de e-mail e documentos PDF de equipes nacionais/governamentais/financeiras de resposta a emergências de computadores (CERTs), fornecedores de TI e comunidades podem ser usados como fonte de IoCs para CyberTrace. A extração de IOCs é possível tanto do corpo quanto do anexo do e-mail (XML, CSV, JSON, PDF). Servidores IMAP/POP3 e pastas locais/compartilhadas com uma coleção de arquivos PDF podem ser usados como fontes de feed.



Páginas com informações detalhadas sobre cada indicador fornecem análises ainda mais profundas. Cada página apresenta todas as informações sobre um indicador de todos os fornecedores de inteligência de ameaças (desduplicação), de modo que os analistas podem discutir ameaças nos comentários e adicionar inteligência de ameaças internas sobre o indicador. Se o indicador foi detectado, as informações sobre as datas de detecção e os links para a lista de detecções ficarão disponíveis.

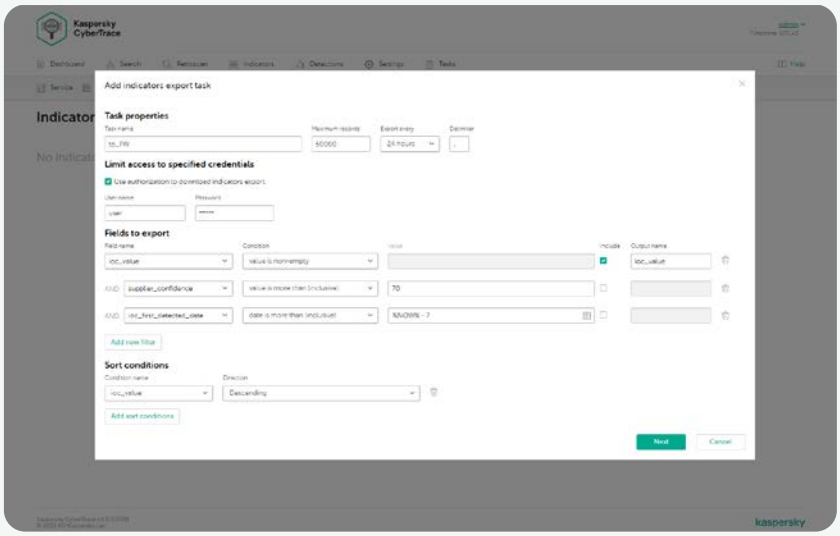
Gráfico de pesquisa

Um Gráfico de pesquisa permite explorar visualmente os dados e as detecções armazenadas no CyberTrace e descobrir semelhanças entre as ameaças. Ele permite a visualização gráfica da relação entre URLs, domínios, IPs, arquivos e outros contextos encontrados durante investigações. O gráfico inclui os seguintes recursos: transformações, minigráfico, nós de agrupamento, adição de links de maneira manual, adição de indicadores e pesquisa por nós no gráfico. O enriquecimento de IoCs no gráfico de pesquisas do VirusTotal é compatível.



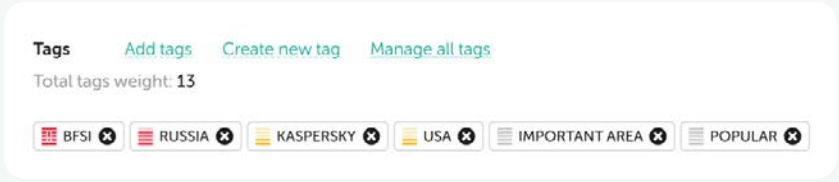
Tarefa de exportação de indicadores

O recurso de exportação de indicadores é compatível com a integração nativa de IoCs com controles de segurança terceirizados, tal como listas de políticas (listas de bloqueios), assim como o compartilhamento de dados de ameaças entre instâncias do Kaspersky CyberTrace ou com outras plataformas de TI.



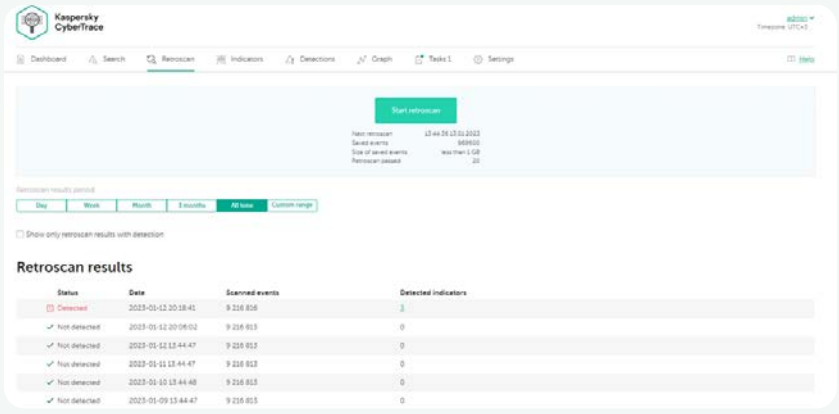
Tags de IoC

Marcar IoCs simplifica seu gerenciamento. É possível criar uma tag, especificar seu peso (importância) e usá-la para marcar IoCs manualmente. Você também pode classificar e filtrar IoCs com base nessas tags e seus pesos.



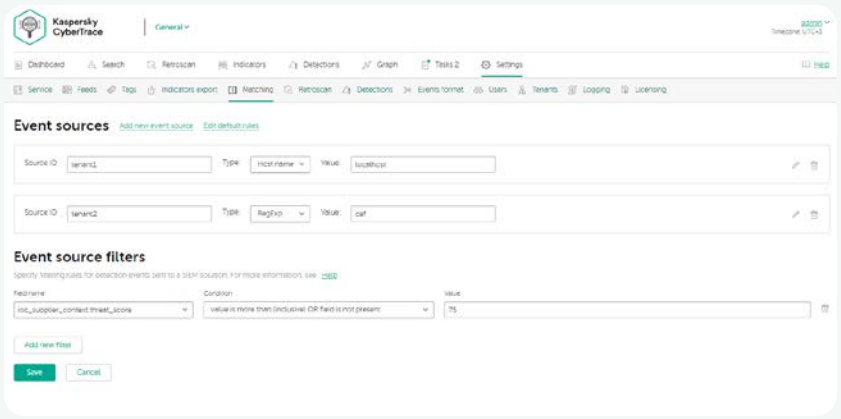
Recurso de retroverificação

Com o recurso de correlação histórica (retroscan), é possível analisar itens observáveis a partir de eventos verificados anteriormente usando os feeds mais recentes para encontrar ameaças previamente descobertas. Todas as detecções históricas são incluídas no relatório para investigação futura.



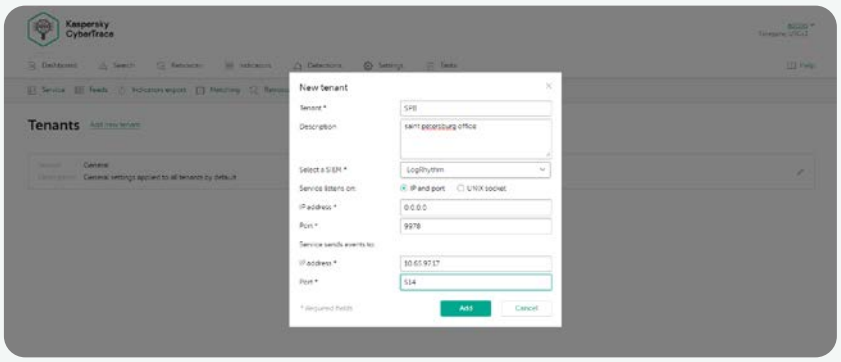
Filtros de origem de evento

Um filtro para enviar eventos de detecção a soluções de SIEM reduz a carga sobre eles e sobre os analistas que enfrentam a fadiga de alertas. Ele permite que você envie ao SIEM apenas as detecções mais perigosas, aquelas que devem ser tratadas como incidentes. Todas as demais detecções ficam salvas no banco de dados interno e podem ser usadas durante análises de causa ou para descoberta de ameaças.



Compatível com multitenancy

Multitenancy é compatível com casos de uso de empresas que fornecem serviços gerenciados de segurança (MSSP) ou de grandes empresas quando um provedor de serviços (escritório central) precisa lidar separadamente com eventos de diferentes filiais (locações). Dessa forma, apenas uma instância do Kaspersky CyberTrace pode ser conectada a diferentes soluções de SIEM a partir de diferentes locações, e você pode configurar quais feeds devem ser usados com cada uma delas.



Matriz de estatísticas de indicador e intersecção de feeds

As estatísticas de uso do feed para medição da efetividade dos feeds integrados e a matriz de intersecção de feeds ajudam a escolher os fornecedores de inteligência de ameaças mais valiosos.

A HTTP RestAPI permite que você pesquise e gerencie a inteligência de ameaças

Ao usar a Rest API, o Kaspersky CyberTrace pode ser facilmente integrado a ambientes complexos para automação e orquestração. Integração com a plataforma de monitoramento, análise e resposta a incidentes.

Outros recursos do produto

- Conectores de SIEM para uma ampla gama de soluções de SIEM para visualizar e gerenciar dados sobre detecções de ameaças
- Pesquisa sob demanda de indicadores (hashes, endereços IP, domínios, URLs) para investigação aprofundada de ameaças
- Filtragem avançada para feeds
- Análise em massa de registros e arquivos
- Interface de linha de comando para plataformas Windows e Linux
- Modo autônomo, onde o Kaspersky CyberTrace recebe e analisa os registros de várias fontes, como dispositivos de rede
- E muito mais

Embora o Kaspersky CyberTrace e o Kaspersky Threat Data Feeds possam ser utilizados separadamente, quando utilizados em conjunto eles reforçam significativamente as suas capacidades de detecção de ameaças, fortalecendo as suas operações de segurança com visibilidade global das ameaças cibernéticas.

Com o Kaspersky CyberTrace e o Kaspersky Threat Data Feeds, as organizações podem:

Destilar e priorizar de forma eficiente os alertas de segurança.

Reduzir o volume de trabalho de analistas e evitar casos de burnout.

Identificar imediatamente alertas críticos e tomar decisões melhores sobre os alertas que devem ser escalados para as equipes de resposta a incidentes

Criar uma defesa proativa e orientada por inteligência.

Kaspersky CyberTrace

Saiba mais

www.kaspersky.com

#kaspersky
#bringonthefuture